Cryptography: A Complete Review

Monika Mishra[1], Shashi Sharma[2], Dr. Varun P saxena[3]
[1]*M.Tech Scholar, Department of Computer Science, Jaipur Institute of Technology, Jaipur (Raj)*
[2]*Assistant Professor, Department of Computer Science, Jaipur Institute of Technology, Jaipur (Raj)*
[3]*Assistant Professor,Govt. Women Engg. Collage, Makhupura, Ajmer,Rajasthan.*

***Abstract*- Security is also desired to be proper in order to data to be shared securely so we have reviewed some cryptographic concept which will be used in our paper to implement the proposed work. Here we have explored the concept of cryptography, Diffie-Hellman, Hash Functions.**

***Index Terms*- Diffie-Hellman, Cryptography, Hash Functions.**

I. INTRODUCTION

Cryptography,[1] or cryptology, is the training and investigation of concealing data. It is at times called code, yet this isn't generally a right name. It is the science used to endeavor to protect data secret and. Present day cryptography is a blend of arithmetic, software engineering, and electrical engineering. Cryptography is utilized as a part of ATM (bank) cards, PC passwords, and shopping on the web.

At the point when a message is sent utilizing cryptography, it is changed (or encoded) before it is sent. The strategy for changing text is known as a "code" or, all the more decisively, a "figure". The changed text is called "ciphertext". The change makes the message hard to peruse. Somebody who needs to peruse it must change it back (or unscramble it). Step by step instructions to transform it back is a secret. Both the individual that sends the message and the one that gets it should know the secret approach to transform it, yet other individuals ought not have the capacity to. Concentrate the cyphertext to find the secret is called "cryptanalysis" or "splitting" or here and there "code breaking".[2][3]

Distinctive sorts of cryptography can be simpler or harder to utilize and can shroud the secret message better or more awful. Ciphers utilize a "key" which is a secret that conceals the secret messages. The cryptographic strategy needn't be secret. Different individuals can utilize a similar technique however extraordinary keys, so they can't read each other's messages. Since the Caesar figure has just the same number of keys as the quantity of letters in the letter set, it is effectively split by attempting all the keys. Ciphers that permit billions of keys are broken by more complex methods.

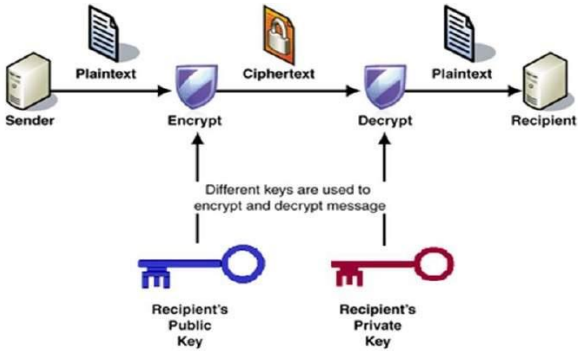

Fig 1. Cryptographic Concept

II. LITERATURE REVIEW

Vaibhav Poonia, Dr. Narendra Singh Yadav, Security has reliably been an amazing worry at whatever point there is correspondence amongst sender and recipient. To beat the issues of security ruptures various cryptographic calculations are utilized like: AES, DES, Triple DES, Blowfish, et cetera. The objective of this paper is to overhaul and evaluate the Blowfish count on the preface of various parameters like Encryption Quality, Correlation Coefficients, Key Sensitivity Test and Size of Output File. Md. Asif Mushtaque and Hash Dhiman ,they proposed our new symmetric key encryption count with decreased space disperse quality (AM Encryption Algorithm-AMEA).According to circle encryption hypothesis an encryption procedure should utilize not exactly or equivalent to the extent of the first document measure. V. Venukumar, proposes Multi-Factor Authentication is used as a foolproof solution to various issues involved in present day critical authentication systems. However, it comes with the

overhead of employing multiple authentication programs to complete the process. Moreover, current multi-factor authentication schemes require all intermediate One Time Passwords(OTPs) to be stored for the lifetime of the authentication process.

III. DIFFIE–HELLMAN KEY EXCHANGE

Diffie– Hellman key exchange (D– H)[nb 1] is a technique for securely trading cryptographic keys over a public channel and was one of the primary public-key protocols as initially conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.[1][2] D– H is one of the most punctual pragmatic cases of public key exchange executed inside the field of cryptography.

Customarily, secure encoded communication between two parties required that they initially exchange keys by some secure physical channel, for example, paper key records transported by a put stock in messenger. The Diffie–Hellman key exchange technique permits two parties that have no earlier information of each other to together set up a common secret key over an insecure channel. This key would then be able to be utilized to scramble ensuing communications utilizing a symmetric key figure.

Diffie–Hellman is utilized to secure an assortment of Internet administrations. In any case, inquire about distributed in October 2015 proposes that the parameters being used for some D– H Internet applications around then are not sufficiently solid to counteract trade off by extremely all around financed attackers, for example, the security administrations of expansive governments. [3]

The plan was first distributed by Whitfield Diffie and Martin Hellman in 1976,[2] yet in 1997 it was uncovered that James H. Ellis,[4] Clifford Cocks and Malcolm J. Williamson of GCHQ, the British signs insight office, had previously[when?] demonstrated how public-key cryptography could be achieved.[5]

Despite the fact that Diffie– Hellman key understanding itself is a non-validated key-assention convention, it gives the premise to an assortment of confirmed protocols, and is utilized to give forward mystery in Transport Layer Security's vaporous modes (alluded to as EDH or DHE relying upon the figure suite).

The strategy was taken after in a matter of seconds a short time later by RSA, a usage of public-key cryptography utilizing unbalanced calculations.

Diffie– Hellman Key Exchange builds up a mutual secret between two parties that can be utilized for secret communication for trading data over a public system. The accompanying theoretical graph shows the general thought of the key exchange by utilizing hues rather than substantial numbers.

The procedure starts by hosting the two gatherings, Alice and Bob, concur on a subjective beginning shading that does not should be kept secret (but rather ought to be distinctive each time [7]); in this case the shading is yellow. Each of them chooses a secret shading that they mind their own business. For this situation, orange and blue-green. The significant piece of the procedure is that Alice and Bob now combine their secret shading with their commonly shared shading, bringing about orange-tan and light-blue blends individually, at that point publicly exchange the two blended hues. At long last, each of the two combine the shading they got from the band together with their own private shading. The outcome is a last shading blend yellow-darker that is indistinguishable to the accomplice's shading blend.

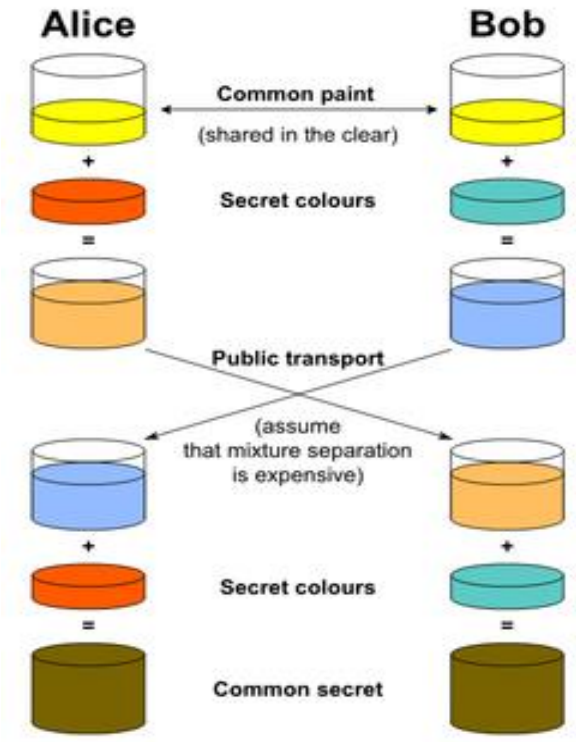

Fig 2. Diffie- Hellman Algorithm

IV. HASH FUNCTIONS

Hash functions are to a great degree helpful and show up in all information security applications.

A hash function is a mathematical function that changes over a numerical input value into another packed numerical value. The input to the hash function is of subjective length yet yield is dependably of fixed length.

Values returned by a hash function are called message process or just hash values. The following picture illustrated hash function −

Features of Hash Functions

The typical features of hash functions are −

Fixed Length Output (Hash Value)

Hash function coverts data of arbitrary length to a fixed length. This procedure is frequently alluded to as hashing the data.

By and large, the hash is significantly littler than the input data, thus hash functions are at times called pressure functions.

Since a hash is a littler portrayal of a larger data, it is likewise alluded to as a process.

Hash function with n bit yield is alluded to as a n-bit hash function. Prevalent hash functions create values in the vicinity of 160 and 512 bits.

Efficiency of Operation

Generally, for any hash function h with input x, computation of h(x) is a fast operation.

Computationally hash functions are much faster than a symmetric encryption.

Properties of Hash Functions

In order to be an effective cryptographic tool, the hash function is desired to possess following properties −

Pre-Image Resistance

This property implies that it ought to be computationally difficult to switch a hash function.

At the end of the day, if a hash function h created a hash value z, at that point it ought to be a troublesome procedure to discover any input value x that hashes to z.

This property secures against an assailant who just has a hash value and is attempting to discover the input.

Second Pre-Image Resistance

This property implies given an input and its hash, it ought to be elusive an alternate input with a similar hash.

As it were, if a hash function h for an input x produces hash value h(x), at that point it ought to be hard to locate some other input value y with the end goal that h(y) = h(x).

This property of hash function secures against an assailant who has an input value and its hash, and needs to substitute distinctive value as legitimate value set up of unique input value.

Collision Resistance

This property implies it ought to be elusive two unique inputs of any length that outcome in a similar hash. This property is additionally alluded to as collision free hash function.

As such, for a hash function h, it is elusive any two distinct inputs x and y with the end goal that h(x) = h(y).

Since, hash function is compressing function with fixed hash length, it is unimaginable for a hash function not to have collisions. This property of collision free just affirms that these collisions ought to be elusive.

This property makes it exceptionally troublesome for an aggressor to discover two input values with a similar hash.

Additionally, if a hash function is collision-resistant then it is second pre-picture resistant.

Popular Hash Functions

Message Digest (MD)

MD5 was most well known and generally utilized hash function for very a few years.

The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was embraced as Internet Standard RFC 1321. It is a 128-piece hash function.

MD5 digests have been broadly utilized as a part of the software world to give affirmation about integrity of exchanged document. For instance, document servers frequently give a pre-registered MD5 checksum for the records, with the goal that a client

can look at the checksum of the downloaded record to it.

In 2004, collisions were found in MD5. A logical assault was accounted for to be effective just in a hour by utilizing PC bunch. This collision assault brought about traded off MD5 and thus it is never again prescribed for utilize.

Secure Hash Function (SHA)

Family of SHA contain four SHA calculations; SHA-0, SHA-1, SHA-2, and SHA-3. Despite the fact that from same family, there are basically unique.

The first form is SHA-0, a 160-piece hash function, was distributed by the National Institute of Standards and Technology (NIST) in 1993. It had couple of shortcomings and did not turn out to be extremely prevalent. Later in 1995, SHA-1 was intended to remedy affirmed shortcomings of SHA-0.

SHA-1 is the most broadly utilized of the current SHA hash functions. It is utilized in a few generally utilized applications and protocols including Secure Socket Layer (SSL) security.

In 2005, a strategy was found for revealing collisions for SHA-1 inside pragmatic time period making long haul employability of SHA-1 farfetched.

SHA-2 family has four further SHA variations, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No effective assaults have yet been accounted for on SHA-2 hash function.

In spite of the fact that SHA-2 is a solid hash function. In spite of the fact that fundamentally unique, its essential outline is still takes after plan of SHA-1. Henceforth, NIST called for new focused hash function plans.

In October 2012, the NIST picked the Keccak calculation as the new SHA-3 standard. Keccak offers many advantages, for example, proficient execution and great protection for assault.

Keys For Comparison	MD5	SHA
Security	Less Secure than SHA	High Secure than MD5
Message Digest Length	128 Bits	160 Bits
Attacks required to find out original Message	2^{128} bit operations required to break	2^{160} bit operations required to break
Attacks to try and find two messages producing the same MD	2^{64} bit operations required to break	2^{80} bit operations required to break
Speed	Faster, only 64 iterations	Slower than MD5, Required 80 iterations
Successful attacks so far	Attacks reported to some extents	No such attach report yet

Fig 3. MD5 and SHA comparison

RIPEMD

The RIPEND is an acronym for RACE Integrity Primitives Evaluation Message Digest. This arrangement of hash functions was composed by open research group and by and large known as a family of European hash functions.

The set incorporates RIPEND, RIPEMD-128, and RIPEMD-160. There additionally exist 256, and 320-piece forms of this calculation.

Unique RIPEMD (128 piece) depends on the plan standards utilized as a part of MD4 and found to give sketchy security. RIPEMD 128-piece rendition came as a convenient solution substitution to beat vulnerabilities on the first RIPEMD.

RIPEMD-160 is an enhanced adaptation and the most generally utilized form in the family. The 256 and 320-piece variants diminish the shot of incidental collision, yet don't have more elevated amounts of security when contrasted with RIPEMD-128 and RIPEMD-160 individually.

Whirlpool

This is a 512-bit hash function.

It is derived from the modified version of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.

Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

V. CONCLUSION

In this paper we have reviews the concepts which we will be implementing for the secure message sending and we have discuss in details the Hash functions, Diffe- Hellman, etc.. and together will using that we will work for forming the strong and secure way of message sending.

REFERENCES

[1] Merkle, Ralph C (April 1978). "Secure Communications Over Insecure Channels". Communications of the ACM. 21 (4): 294–299. doi:10.1145/359460.359473. Received August, 1975; revised September 1977

[2] Jump up to: a b Diffie, W.; Hellman, M. (1976). "New directions in cryptography" (PDF). IEEE

Transactions on Information Theory. 22 (6): 644–654. doi:10.1109/TIT.1976.1055638.

[3] Jump up to: a b c d e Adrian, David; Bhargavan, Karthikeyan; Durumeric, Zakir; Gaudry, Pierrick; Green, Matthew; Halderman, J. Alex; Heninger, Nadia; Springall, Drew; Thomé, Emmanuel; Valenta, Luke; VanderSloot, Benjamin; Wustrow, Eric; Zanella-Béguelin, Santiago; Zimmermann, Paul (October 2015). "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" (PDF).

[4] Jump u Ellis, J. H. (January 1970). "The possibility of Non-Secret digital encryption" (PDF). CESG Research Report. Archived from the original (PDF) on 2014-10-30. Retrieved 2015-08-28.

[5] Jump up "GCHQ trio recognised for key to secure shopping online". BBC News. 5 October 2010. Retrieved 5 August 2014.

[6] Jump up Hellman, Martin E. (May 2002), "An overview of public key cryptography" (PDF), IEEE Communications Magazine, 40 (5): 42–49, doi:10.1109/MCOM.2002.1006971

[7] Jump up to: a b "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" (PDF). Retrieved 30 October 2015.

[8] Jump up Garzia, F. (2013), Handbook of Communications Security, WIT Press, p. 182, ISBN 1845647688

[9] Jump up Buchanan, Bill, "Diffie-Hellman Example in ASP.NET", Bill's Security Tips, retrieved 2015-08-27

[10] Jump up Buchmann, Johannes A. (2013), Introduction to Cryptography (2nd ed.), Springer Science & Business Media, pp. 190–191, ISBN 1441990038

[11] Jump up Barbulescu, Razvan; Gaudry, Pierrick; Joux, Antoine; Thomé, Emmanuel (2014). "A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic". Advances in Cryptology – EUROCRYPT 2014. Proceedings 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science. 8441. Copenhagen, Denmark. pp. 1–16. ISBN 978-3-642-55220-5. doi:10.1007/978-3-642-55220-5_1.

[12] Jump up C. Kaufman (Microsoft) (December 2005). "RFC 4306 Internet Key Exchange (IKEv2) Protocol". Internet Engineering Task Force (IETF).

[13] Jump up Whitfield Diffie, Paul C. Van Oorschot, and Michael J. Wiener "Authentication and Authenticated Key Exchanges", in Designs, Codes and Cryptography, 2, 107-125 (1992), Section 5.2, available as Appendix B to U.S. Patent 5,724,425